5 FAH-2 H-860
ANTI-VIRUS PROGRAM

(TL:TEL-2;   05-23-2002)

5 FAH-2 H-861 POLICY

(TL:TEL-2;   05-23-2002)
(Uniform all agencies)

a. In accordance with 12 FAM 643.2-9, all systems connected to Department networks must be protected with virus detection and prevention programs. IRM/OPS/ITI/SI/IIB (Systems Integrity Division, Information Integrity Branch) provides anti-virus software and documentation to all bureaus and field posts free of charge. The software includes initial and updated definition files for IBM compatible and Macintosh systems operating the full range of Microsoft environments. The Setup and Installation Procedures Handbook answers procedural questions about installation. Contact IRM/OPS/ITI/SI/IIB at (202) 203-5003 for more information.

b. Anti-virus software may be obtained and installed from the bureau or post's systems offices abroad by Department of State, or employed contractor personnel, while they are employed with the Department, for home usage to prevent malicious code from migrating to the office environment. Diplomatic privilege and various host country custom laws prohibit Foreign Service National (FSN) or Third Country Nationals (TCN) from removing or installing Department of State procured anti-virus software on privately owned PCs. Licensing, reproduction, and distribution of anti-virus software for domestic and posts usage abroad is the responsibility of the Anti-Virus Program Staff, IRM/OPS/ITI/SI/IIB. IPC personnel must install and update anti-virus software on all computers maintained by the IPC, i.e., TEMPEST computers and non-TEMPEST classified computers within controlled access areas (CAAs).

5 FAH-2 H-862 UNCLASSIFIED SYSTEMS

(TL:TEL-2;   05-23-2002)
(Uniform all agencies)

a. DS/IST/ACD (Diplomatic Security, Information Security Technology, Assessment and Certification Division) authorizes systems personnel to update virus definition files from the anti-virus software vendor's Internet bulletin board or web-site via dial-up modem installed on an unclassified, stand-alone computer only. The computer may not be connected to or be a part of any LAN. The definition update files should be downloaded to a clean floppy diskette or CD-ROM that contains no sensitive information. The standalone computer's hard drive must be scanned prior and subsequent to accessing the bulletin board or web-site. Scan the floppy diskette before use on any other USG computer. Use the clean floppy or CD-ROM to copy the definition update files to all other unclassified computers. Virus definition files and Scanmail virus pattern and engine updates may also be downloaded directly from the Intranet IRM web pages.

b. At critical threat posts, all software for use on unclassified systems within the CAA must be procured via secure channels. Virus definition files and ScanMail virus pattern and engine updates may also be downloaded directly from the Intranet IRM web pages. Downloading of virus definition update files for these systems from the Internet is prohibited. Follow the guidelines listed below.

5 FAH-2 H-863 CLASSIFIED SYSTEMS

(TL:TEL-2; 05-23-2002)
(Uniform all agencies)

Downloading of updated virus definition files from the Internet or Internet based bulletin boards for classified systems is STRICTLY PROHIBITED. Definition files and ScanMail virus pattern and engine updates may be downloaded from the Intranet IRM web pages for use on classified systems or for unclassified systems described in 5 FAH-2 H-862 b. For all posts abroad, IRM/OPS/ITI/SI will send original program and updated anti-virus definition files via classified pouch in the care of the Information Programs Officer (IPO), Information Management Officer (IMO) or a cleared U.S. citizen employee. The Department supplied CD-ROM disk or media containing anti-virus software obtained from the Intranet IRM web pages, must be labeled with the highest classification of material processed, and once used, this media cannot be returned for unclassified use.

5 FAH-2 H-864 VIRUS INCIDENT REPORTING

(TL:TEL-2; 05-23-2002)
(Uniform all agencies)

If a virus is discovered, send an official telegram or memorandum to the Department for IRM/OPS/ITI/SI/IIB and DS/IST/ACD. The report should include the following:

(1) Name of virus and occurrences;

(2) Location of virus (bureau, post or office);

(3) Origin of virus infection;

(4) Infected equipment type (stand-alone, LANs or network);

(5) Type of software used to eradicate the virus;

(a) Norton Anti-Virus or ScanMail for Exchange Server

(b) NAV Installed Definition Update Files Date:

(c) ScanMail's Installed Virus Pattern and Scan Engine:

(6) Losses incurred (defined as loss of equipment, software or computer system downtime);

(7) Point of contact for follow-up support; and

(8) Remarks.

5 FAH-2 H-865 THROUGH H-869 UNASSIGNED